REMARKS

By this Amendment, claims 1 and 73 have been amended without any intention of narrowing the scope of any of the claims. Applicant has amended the currently pending claims in order to expedite prosecution and does not, by this amendment, intend to abandon subject matter of the claims as originally filed or later presented. Moreover, Applicant reserves the right to pursue such subject matter in a continuing application. Claims 1, 18-21, 72-84 and 109-131 are pending in this patent application. Reconsideration of the rejections in view of the remarks below is requested.

Rejection under 35 U.S.C. §112

The Office Action rejected claims 1, 18-21, 72-78 and 116-129 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant respectfully traverses.

While Applicant expressly disagrees with the rejection and objects to its late presentation since, for example, claim 1 has been examined at least 3 times before this Office Action without any question about its indefiniteness, Applicant has amended claims 1 and 73 without any intention of narrowing the scope of any of the claims and indeed has broadened the scope of the claims.

With respect to claim 1, for example, Applicant submits that that claim clearly and consistently provides that, in response to the recited digital signing, the recipient is permitted to utilize the recited public key and that prior to the digital signing, utilization of the public key is denied. So, in one example embodiment, the public key is not distributed to the recipient unless the recipient performs the digital signing. See, e.g., Applicant's specification, page 35, lines 24-33. In another example embodiment, a secure device contains the public key but the recipient cannot utilize the public key, i.e., the public key cannot be obtained from the secure device, until the recipient performs the digital signing. See, e.g., claim 18.

Applicant submits there is no inconsistency with the claimed permitting use of the public key and the claimed denying utilization of the public key. The permitting use and denying utilization simply occur at two different times divided by a condition, i.e., utilization of the key is not permitted until the claimed digital signing when thereafter the key may be utilized.

Therefore, for at least the above reasons, Applicant respectfully submits that the rejection under 35 U.S.C. §112 of claims 1, 18-21, 72-78 and 116-129 should be withdrawn and the claims be allowed.

Rejection under 35 U.S.C. §103 in view of Muftic and Ding

The Office Action rejected claims 1, 21, 72, 73, 77, 78, 116-120, 129 and 130 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,745,574 ("Muftic") in view of the article titled "Undetectable On-Line Password Guessing Attacks", ACM SIGOPS Operating Systems Review, Vol. 29, Issue 3 (October 1995) by Ding et al. ("Ding"). Applicant respectfully traverses the rejection, without prejudice.

Muftic discloses a system that may have the ability to provide efficient key management and distribution in a secure manner by several different ways, more effective than existing models, and in a manner which protects public keys from tampering. (Muftic, col. 4, line 65 to col. 5, line 2). Muftic discloses that certification begins with a message sent from the station desiring certification to the certifying authority or by receiving that notification in any other way. Typically, this is done in a Certificate_Signature_Request message. The format of the Certificate_Signature_Request includes a certificate filled in with at least the public key which the requesting entity desires to have certified. The submission may be self-signed using the requestor's private key and transmitted to the CA for signature. When the CA receives the Certificate_Signature_Request, the information contained therein is validated in accordance with the policies established by a policy certification authority, and if the information is correct, the certifying authority issues a Certificate_Signature_Reply message returning to the requesting entity a signed certificate. When the requesting entity receives the Certificate_Signature_Reply message, it undertakes a Receive_Certificate process which verifies the signature on the certificate and stores it in a local certificate data base after verifying that the public key contained in the certificate corresponds to the entity's private key. (Muftic, col. 11, lines 29-53). To verify the signature, the requesting entity has the public key of the certification authority. (Muftic, col. 12, lines 23-43).

The certification authority vouches for the identity of the public key owner, for the integrity of the public key itself, for the binding between the public key and the owner's identity, and optionally for some additional capabilities of the certificate owner in the electronic environment. This guarantee is reflected in the certificate through the identity of the authority, together with the authority's digital signature to the certificate. The signed certificates further may contain references to the types and purposes of public keys, to the

relevant certification policies and eventually to the authorization privileges of certificate owners. (Muftic, col. 10, lines 45-55).

However, the cited portions of Muftic fail to disclose, teach or suggest, *inter alia,* digitally signing said at least one message, by which said recipient agrees to said rules, and in response to said digital signing, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization of said public key as recited in claim 1. Similarly, the cited portions of Muftic fail to disclose, teach or suggest, *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key and prior to said recipient digitally signing said message, denying use of said public key as recited in claim 73.

The Office Action states that "Muftic discloses providing the recipient with at least one message containing the rules of the system including a rule regarding maintaining secrecy of public key in (column 10 lines 52-57). Muftic discloses digitally signing by recipient at least one message which recipient agrees to rules and permitting recipient to utilize public key in (column 11 lines 29-53; column 12 lines 32-40)." Applicant respectfully disagrees.

In those citations (col. 10, lines 52-57, col. 11, lines 29-53 and col. 12, lines 32-40), Muftic merely discloses the nature of a certificate from a certifying authority and the process of requesting such a certificate from the certifying authority. As discussed above, the certificates are requested by forwarding a public key and thus the certificate requestor already has access to or use of a public key. Further, the acceptance or denial of a certificate does not effect a permission of a recipient to utilize a public key. The certificate requestor in Muftic already has access to or use of the public key.

The Office Action states "[t]he certificate itself is signed; and therefore agrees to the purposes if [sic] the key. The purposes of a key implicitly include keeping the key secret." Respectfully, signing of a certificate in Muftic provides no indication of the acceptance of rules applying to a key nor does it effect a permission of a recipient to utilize a public key. In Muftic, a certificate is merely a representation by the certifying authority of, for example, of the association between the identity of a person and a public key (e.g., certifying that a certain public key is associated with a certain person). The signing of that certificate by the certifying authority in Muftic is merely a mechanism to help ensure to the recipient of the certificate that the certificate came from the certifying authority (e.g., just as a person would apply a handwritten signature to a letter to a recipient, rather than send a letter unsigned).

Therefore, the signing by the certifying authority of the certificate in Muftic simply does not trigger that a recipient can start utilizing a public key; indeed, the recipient in Muftic already utilizes the public key (e.g., the recipient uses it to request the certificate in the first place). Moreover, the purpose of a key does not implicitly include keeping the key secret. In prior art public key cryptography systems, the public key is not kept secret. The point of those systems is to allow exchange of encrypted messages without having to share secret keys; the public key is freely available and open to the public. So while Applicant would agree that a private key is intended to be kept secret, Applicant disagrees with the general statement and particularly in respect to public keys.

Thus, the cited portions of Muftic fail to at least disclose, teach or suggest, *inter alia*, digitally signing said at least one message, by which said recipient agrees to said rules, and in response to said digital signing, permitting said recipient to utilize said public key as recited in claim 1 or in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73.

Further, assuming *arguendo* that Muftic and Ding are properly combinable (which Applicant does not concede and disagrees that they are), Applicant submits that the cited portions of Ding fail to overcome the shortcomings of Muftic.

The cited portions of Ding merely disclose a server S, providing to client A, a public key generated for A. The cited portions of Ding, however for example, fail to disclose, teach or suggest, *inter alia,* digitally signing said at least one message, by which said recipient agrees to rules including a rule regarding maintaining secrecy of said public key, let alone in response to said digital signing, permitting said recipient to utilize said public key and prior to said digital signing, denying utilization of said public key as recited in claim 1. Similarly, the cited portions of Ding fail to disclose, teach or suggest, *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key and prior to said recipient digitally signing said message, denying use of said public key as recited in claim 73.

Therefore, for at least the above reasons, the cited portions of Muftic fail to disclose, teach or suggest all the features recited by claims 1 and 73. Claims 21, 72, 77, 78, 116-120, 129 and 130 depend from claims 1 and 73 respectively and are thus patentable at least for the same reasons as claims 1 and 73 respectively, and for the additional features recited therein. As a result, Applicant respectfully submits that the rejection under 35 U.S.C. §102(e) of

claims 1, 21, 72, 73, 77, 78, 116-120, 129 and 130 based on Muftic should be withdrawn and the claims be allowed.

Rejection under 35 U.S.C. §103 in view of Muftic, Ding and Curry

The Office Action rejected claims 18, 20, 74, 121-125, 127, 128 and 131 under 35 U.S.C. §103(a) as being obvious in view of Muftic, further in view of Ding and further in view of U.S. Patent No. 5,940,510 to Curry et al. ("Curry"). Applicant respectfully traverses the rejection, without prejudice.

For at least the reasons discussed above, claims 1 and 73 are patentable over the cited portions of Muftic and Ding.

Further, assuming *arguendo* that Curry is properly combinable with Muftic and Ding (which Applicant does not concede and disagrees that they are), the cited portions of Curry do not overcome the shortcomings of Muftic and Ding, or vice versa. Curry merely disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry, col. 4, lines 49-52).

The cited portions of Curry alone or in combination with Muftic and Ding, however, fail to disclose, teach or suggest, *inter alia,* denying access to a public key and in response to a digital signing, permitting a recipient to utilize said public key as recited in claim 1 or *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73.

Claims 18, 20, 74, 121-125, 127, 128 and 131 depend from claims 1 and 73 respectively and are, therefore, patentable over Muftic, Ding and Curry for at least the same reasons as provided above in respect of claims 1 and 73 respectively above, and for the additional features recited therein.

Therefore, for at least the above reasons, the cited portions of Muftic, Ding and Curry fail to disclose, teach or suggest all the features recited by claims 18, 20, 74, 121-125, 127, 128 and 131. As a result, Applicant respectfully submits that the rejection of claims 18, 20, 74, 121-125, 127, 128 and 131 under 35 U.S.C. §103(a) in view of Muftic, Ding and Curry should be withdrawn and the claims be allowed.

Rejection under 35 U.S.C. §103 in view of Muftic and Curry

The Office Action rejected claims 79, 80, 83, 84 and 109-115 under 35 U.S.C. §103(a) as being obvious in view of Muftic and further in view of Curry. Applicant respectfully traverses the rejection, without prejudice.

Applicant submits that claim 79 is patentable over the cited portions of Muftic alone at least because the cited portions of Muftic fail to disclose, teach or suggest a method of enforcing a security policy in a cryptographic system comprising, *inter alia*, providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device. The citations to col. 15, lines 32-43 and col. 12, lines 60-64 of Muftic are inapposite. In those citations, Muftic merely discloses a certifying authority re-signing a certificate, which involves a certifying authority generating a new key pair for generating the certificate. Those citations fail to provide any disclosure, teaching or suggesting regarding an inactive public key, let alone about a secure device containing the inactive public key and from which the public key cannot be obtained or about activating the public key.

Further, Applicant submits that the cited portions of Curry do not overcome the shortcomings of Muftic, or vice versa. Curry merely disclose a secure device that may have the ability to store or create a private/public key set, whereby the private key never leaves the secure device and is not revealed under almost any circumstance. (Curry, col. 4, lines 49-52).

Thus, the cited portions of Curry alone or in combination with Muftic, however, fail to disclose, teach or suggest, *inter alia,* providing a recipient with a message containing rules of said system and with a secure device containing an inactive form of said public key, wherein said public key cannot be obtained from said device, and in response to said recipient digitally signing said message, activating said public key in said secure device as recited in claim 79.

Claims 80, 83, 84 and 109-115 depend from claim 79 and are thus patentable at least for the same reasons as claim 79, and for the additional features recited therein.

Therefore, for at least the above reasons, the cited portions of Muftic and Curry fail to disclose, teach or suggest all the features recited by claims 79, 80, 83, 84 and 109-115. As a result, Applicant respectfully submits that the rejection of claims 79, 80, 83, 84 and 109-115 under 35 U.S.C. §103(a) in view of Muftic and Curry should be withdrawn and the claims be allowed.

Rejection under 35 U.S.C. §103 in view of Muftic, Ding, Curry and Ryder

The Office Action rejected claim 126 under 35 U.S.C. §103(a) as being obvious in view of Muftic, further in view of Ding, further in view of Curry and further in view of U.S. Patent No. 4,953,209 to Ryder ("Ryder"). Applicant respectfully traverses the rejection, without prejudice.

For at least the reasons discussed above, claim 73 is patentable over the cited portions of Muftic, Ding and Curry.

Further, assuming *arguendo* that Ryder is properly combinable with Muftic, Ding and Curry (which Applicant does not concede and disagrees that they are), the cited portions of Ryder do not overcome the shortcomings of Muftic, Ding and Curry, or vice versa. Ryder merely discloses a system for electronically transmitting data objects such as computer programs with a means for verifying that the computer program was actually received and the terms and conditions of its use accepted by the receiver is presented. (Ryder, Abstract).

The cited portions of Ryder alone or in combination with Muftic, Ding and Curry, however, fail to disclose, teach or suggest, *inter alia,* in response to said recipient digitally signing said message, by which said recipient agrees to said rules, permitting said recipient to utilize said public key as recited in claim 73. For example, Ryder simply has no disclosure, teaching or suggestion regarding a public key.

Claim 126 depends from claim 73 and is, therefore, patentable over Muftic, Ding, Curry and Ryder for at least the same reasons as provided above in respect of claim 73, and for the additional features recited therein.

Therefore, for at least the above reasons, the cited portions of Muftic, Ding, Curry and Ryder fail to disclose, teach or suggest all the features recited by claim 126. As a result, Applicant respectfully submits that the rejection of claim 126 under 35 U.S.C. §103(a) in view Muftic, Ding, Curry and Ryder should be withdrawn and the claim be allowed.

All rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance. If questions relating to patentability remain, the Examiner is invited to contact the undersigned to discuss them.

Should any fees be due, please charge them to our deposit account no. 03-3975, under our order no. 061047/0264493. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced deposit account.

Respectfully submitted,

PILLSBURY WINTHROP SHAW PITTMAN LLP

#54248

Christophe LAIK

for Jean-Paul G. Hoffman
Reg. No. 42,663
Tel. No. 703-770-7794
Fax No. 703-770-7901

P. O. Box 10500
McLean, VA 22102
(703) 770-7900